UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/650,440	08/27/2003	Frederic G. Thiele	END920030068US1	7247

26502 7590 06/07/2011

IBM CORPORATION
IPLAW SHCB/40-3
1701 NORTH STREET
ENDICOTT, NY 13760

EXAMINER	
PERUNGAVOOR, VENKATANARAY	
ART UNIT	**PAPER NUMBER**
2432	
NOTIFICATION DATE	**DELIVERY MODE**
06/07/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

endiplaw@us.ibm.com

Office Action Summary	**Application No.**	**Applicant(s)**	
	10/650,440	THIELE ET AL.	
	Examiner	**Art Unit**	
	VENKAT PERUNGAVOOR	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 May 2011*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12,21-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *21-24* is/are allowed.

6)☒ Claim(s) *1-8,12 and 25-28* is/are rejected.

7)☒ Claim(s) *9-11* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 5/2/2011 has been entered.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 1, 3-4,6-7, 12, 25, 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 59941881 to Conklin et al.(hereinafter Conklin) in view of US Patent Pub 2003/0212821 to Gillies et al.(hereinafter Gillies).

Regarding Claim 1, 25, Conklin discloses a computer program product for automatically determining if a packet is a new, exploit candidate, the computer program product comprising:

a computer--readable tangible storage_device see Col 3 LN 15-21;

first program instructions to determine if the packet is a known exploit see Col 7 Ln 44-50;

third program instructions to determine if the packet is network administration traffic see Col 3 Ln 8-11(where the type of packet can include telnet which includes network administration);

fourth program instructions, responsive to the packet being a known exploit OR the packet_being of network administration traffic to determine that the packet is not a new, exploit candidate see Col 7 Ln 50-60; and

fifth program instructions, responsive to the packet not being a known exploit see Fig. 7 item "Attack Check 1" & "Perform next check"; AND the packet not being network administration traffic AND or-the packet not_being another type of traffic known to be benign, to determine and report that the packet is a new, exploit candidate see Fig. 6 item "Reportable Activity" & "Event Log Analyzer"; and wherein

the first, second, third, fourth and fifth program instructions are stored on the computer-readable tangible_storage device see Col 3 Ln 28-35.

But Conklin does not disclose the packet addressed to a broadcast address. However, Gillies discloses the packet addressed to a broadcast address see Par. 0052-0053.

It would be obvious to one having ordinary skill in the art at the time of the invention to include the packet being a broadcast address in the invention of Conklin in order to forward routing information to other devices as taught in Gillies see Par. 0023.

Regarding Claim 3. Conklin discloses wherein the first program instructions determine if the packet is a known exploit by searching the packet for a known signature of a known exploit see Col 7 Ln 50-55.

Regarding Claim 4 Conklin discloses wherein the first program instructions determine if the packet is a known exploit by comparing an identity of the packet to one or more identities, sent by an intrusion detection system, of respective packet(s) which the intrusion detection system determined to contain a known exploit see Fig. 7 Attack data.

Regarding Claim 6. Conklin discloses sixth program instructions, responsive to the fifth program instructions determining that the packet is a new exploit candidate, to determine a signature of the packet and report the new exploit candidate and the signature to an administrator see Fig. 6 item “Reportable Activity”; and wherein the sixth program instructions are stored on the computer- readable tangible storage device see Col 3 Ln 15-21.

Regarding Claim 7, 28, Conklin discloses wherein responsive to the fourth program instructions determining that the packet is not a new, exploit candidate, then-a signature of the packet not being determined see Fig. 7 item "Store Packet Statistics" & Fig. 7 " Perform Next check"(the series of checks being done to determine whether the attack is known if none attack type is found then a new attack is log and collected see 29-50).

Regarding Claim 12. Conklin discloses sixth program instructions, responsive to the packet not being a known exploit AND the packet not being network broadcast traffic AND the packet not addressed to a broadcast IP address of a network AND the packet not being another type of traffic known to be benign, to identify a sequence of packets including the first said packet, the sequence of packets being a new, exploit candidate see Fig. 7 item "Store Packet Statistics" & Fig. 7 " Perform Next check"(the series of checks being done to determine whether the attack is known if none attack type is found then a new attack is log and collected see 29-50); and wherein
the sixth program instructions are stored embodied on the computer- readable tangible storage device see Col 3 Ln 15-21.

Claim 2, 26 rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 59941881 to Conklin et al.(hereinafter Conklin) in view of US Patent Pub 2003/0212821 to Gillies et al.(hereinafter Gillies) as applied to claim 1 above, and further in view of US Patent Pub 2003/0225722 to Brown et al.(hereinafter Brown).

Regarding Claim 2, 26 Conklin discloses the series of determination for attacks Fig. 7 item "attack check 1" & "attack type 2" & "attack n" and determining whether it is a known exploit see Col 7 Ln 50-60. Gillies discloses the broadcast packet see Par. 0052-0053. Conklin nor Gillies disclose a web crawler. However, Brown discloses sixth program instructions to determine if the packet is web crawler traffic see Par. 0040 & Par. 0045.

It would be obvious to one having ordinary skill in the art at the time of the invention to include a web crawler determination in the invention of Conklin in order to prevent crawler from extracting information from documents as taught in Brown see Par. 0038.

Claim 5, 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 59941881 to Conklin et al.(hereinafter Conklin) in view of US Patent Pub 2003/0212821 to Gillies et al.(hereinafter Gillies) as applied to claim above, and further in view of US Patent Pub 2004/0078592 to Fagone et al.

Regarding Claim 5, 27, Conklin nor Gillies disclose a honeypot address. However, Fagone discloses wherein the packet was received by a honeypot_computing device at an unused IPaddress, and the computer program product is installed and_executed at the honeypot computing device see Fig. 2 item 203.

It would be obvious to one having ordinary skill in the art at the time of the invention to include a honeypot address in the invention of Conklin in order to track and log all activities of attacker as taught in Fagone see Par. 0016.

Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 59941881 to Conklin et al.(hereinafter Conklin) in view of US Patent Pub 2003/0212821 to Gillies et al.(hereinafter Gillies as applied to claim 1 above, and further in view of US Patent 6185623 to Bailey et al.(hereinafter Bailey).

Regarding Claim 8. Conklin nor Gillies discloses the packet being a broadcast address comparing destination address to the gateway. However, Bailey discloses the second program instructions determine if the packet is addressed to a broadcast IP address of the network by comparing a destination IP address of the packet to a gateway IP address of the network and an netmask of the network which identifies a broadcast IP address of the network see Col 8 Ln 15 -28 & Abstract.

It would be obvious to one having ordinary skill in the art at the time of the invention to include the packet being addressed to broadcast address and comparing destination address to gateway address in the invention of Conklin in order to have one port and pathway to multicast the message as taught in Bailey see Col 7 Ln 35-42.

Allowable Subject Matter

Claim 9-11, 21-24 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

With regard to Claim 21-24, the claims recite a list of protocols determined to be harmless broadcast traffic is not found in prior art nor obvious over prior art.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to VENKAT PERUNGAVOOR whose telephone number is (571)272-7213. The examiner can normally be reached on 8:00-4:30. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/VENKAT PERUNGAVOOR/
Examiner, Art Unit 2432
May 26, 2011